UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,728	10/31/2001	Richard Paul Tarquini	10017270-1	3625

7590 09/22/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/001,728	TARQUINI ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on June 27, 2005.

Claims 1-13 are pending.

Response to Arguments

2. Applicant's argument filed on June 27, 2005 have been fully considered but they are not persuasive.

There are two independent claims in particular claims 1 and 11.

The first argument by the applicant is with regard to the independent claim 1. Applicant argued that claim 1 includes limitations that are not shown or suggested/anticipated by the references on the record, namely **Kouznetsov.**

Applicant wrote the following in support of his argument, independent

Claim 1 recites **a mobile device operable in mobile telecommunication** network having "memory module" and "an operating system" operableto execute an intrusion detection application stored in the memory module." Applicants respectfully submit that Kouznetsov does not disclose or even suggest intrusion detection application stored in the memory module" of a mobile device operable in a mobile telecommunications network" as recited by independent Claim 1, nor has the Examiner explicitly identified any such disclosure in Kouznetsov. Thus, for at least this reason, Kouznetsov does not anticipate independent Claim 1.

Examiner disagrees with this argument, what is argued by the applicant is the limitation which is part of preamble but was not part of the body of the claim 1.

An intended use clause found in the preamble is not afforded the effect of a distinguishing limitation unless the body of the claim sets forth structure which

refers back to, is defined by, or otherwise draws life and breath from the preamble. See In re Casey, 152 USPQ 235 (CCPA 1967)

The second argument by the applicant is with regard to the independent claim 11. Applicant argued that claim 11 includes limitations that are not shown by the combination of Holland and Smaha. Applicant recites the following in support of his argument.

Smaha appears to disclose that information such as log records and audit records are converted to an "event" (defined as "an instant security state of the system" at column 5, lines 7-8 of Smaha), and then Smaha compares the event to a signature. In contrast, Claim 11 recites an intrusion protection system management application . . . operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature" (emphasis added).

Accordingly, neither the portion of Smaha referred to by the Examiner nor elsewhere in Smaha appears to disclose, teach or suggest at least this limitation of Claim 11. To the contrary, in Smaha, the "convert to event" corresponding to reference numeral 144 of Smaha referred to by the Examiner is clearly not a network-exploit rule nor is the information referred to by the Examiner "converted ...into a signature file comprising machine-readable logic representative of an exploit-signature" as recited by Claim 11 .

Examiner disagrees with this argument and would point out that **Smah** discloses

An application operable to receive text-file input defining a network-exploit [figure 1, ref. Num "20" and "12"; figure 5a, ref.Num "12"; column 4, lines 40-49] (For instance, input mechanism shown on figure 1, ref.

Num "20" receives input from any wide array of sources for example user devices shown on figure 1, ref. Num "22") and **convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, [figure 5a, ref. Num "144"; column 5, lines 10-12; Column 6, lines 9-11]** (The misuse engine shown on figure 1, ref. Num "30" converts the input into events/signature and compare it with the known signatures and generate a signature representative of an exploit-signature when detecting a misuse during processing operations and send it to the out put mechanism as shown on figure 5a, ref. Num "32")

Smaha further discloses, " **A signature is the set of events and transition functions that define the sequence of actions that form a misuse**.[see column 5, lines 10-12]. Furthermore Smaha discloses **"Misuse engine 30 uses these events to determine the existence of an actual processing system misuse. Before misuse engine 30 begins processing, however, input mechanism 20 for selectable misuses permits narrowing the scope of analysis to a specified set of misuses meets the recitation that input mechanism sets a network-exploit rule. If this rule are not set, the converting process would not follow. Misuse engine 30 then begins converting process inputs 12 into events and compares the events to signatures[see column 6, lines 9-11] meets the limitation of converting the text file input into a signature file" [See column 6, lines 9-11]. The fact that the input are converted in to events is explicitly disclosed, then if these events were not equivalent to signature file they would not have been able to be compared with signature files.**

The last argument by the applicant is with regard to the independent claim 11.

Applicants respectfully submit that neither Holland nor Smaha, alone or in combination, appears to disclose, teach or suggest that the node is operable to transmit the signature file to mobile device over a radio frequency link" as recited by Claim.

Examiner disagrees with this argument and would point out that **Smah** discloses the following on column 6, lines 9-21].

Misuse engine 30 then begins converting process inputs 12 into events and compares the events to signatures. Misuse engine 30 generates a misuse output upon detecting a misuse during processing system operation. The misuse output consists of two outputs. One output is output signal 32 which misuse engine 30 may send through output signal mechanism 32 to one or more of storage device 34, network 36, communications link 38 and computer memory device 40. The other possible output from misuse engine 30 goes to output report mechanism 38. Output report mechanism 38 may send output reports to one or more of storage device 44, **communications link 46, network 48, meets the limitation transmitting signature file to the mobile device over a radio frequence link.**

For detailed explanation see the office action below.

The rest of the argument by the applicant is with regard to the dependent claims. Applicant argued that the rest of the dependent claims are allowable for the reason that Holland does not disclose the limitation of claims 1, 8 and 11.

In response to the above argument by the applicant, the examiner response discussed for the independent claims above is also valid towards this argument. Therefore all the elements of the limitations is explicitly/implicitly/inherently suggested and disclosed by primary reference "Holland" or by the combinations of the references on the records namely, "Holland" and "Moran" and the rejection remains valid.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1 and 3-10** are rejected under 35 U.S.C. 102(e) as being anticipated by **Victor Kouznetsov** (hereinafter referred as **Kouznetsov**) (U.S. Patent No 6,725,377B1)

5. **As per claim 1 and 9-10, Kouznetsov** a mobile device operable in a mobile telecommunications network, comprising:

- **A memory module for storing data in machine readable format for retrieval and execution by a central processing unit**; [Column 1, lines 53-55;column 4, lines 43-47; column 4, lines 63-65; column 6, lines 58-61; column 10, lines 19-22] (The anti-intrusion software program which

is stored on the CD-ROM or floppy disk is installed on any computer/server by the system administrator as explained on column 4, lines 43-47 and column 4, lines 53-55 and the system administrator is required to retrieve and install the latest versions of updates for each servers. Therefore, inherently, this program is installed in the computers memory and any computer larger or small, must have a central processing unit for execution of this software program installed in its memory module.)

- **An operating system operable to execute an intrusion detection application stored in the memory module.**[Column 6, lines 32-34;column 7, lines 46-48;column 2, lines 39-41] (First as explained on column 2, lines 25-26 and column 2, lines 32-35 it has been disclosed that the **CyberCop Network** which is the real time intrusion detection application software is offered in a variety of outlets and forms. It is accompanied by documentation including the **CyberCop Network** for windows NT version 2 **operating system**. The anti-intrusion monitor server which has stored the intrusion application software manually by the administrator in its own memory module as explained on column 4, lines 43-47, performd program execution using Pentium based server running Window NT operating system as explained on column 6, lines 32-34].

6. **As per claim 3, Kouznetsov** discloses the device as applied to claim 1 above. Furthermore **Kouznetsov** discloses the device wherein the intrusion detection application further comprises an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file and pass the signature file to the associative process engine, the

associative process engine operable to analyze a data packet with the signature file. [Figure 2, column 7, lines 31-38] (The intrusion application which is first loaded at central anti-intrusion server shown at figure 5, ref. Num "514" transmits the modified attack/pattern or signature file to the push administration and the push administration transmit the modified attack/pattern or signature to the anti-intrusion server shown on figure 2, ref. Num "202" meets the recitation of the claim.)

7. **As per claim 4, Kouznetsov** discloses the device as applied to claim 1 above. Furthermore **Kouznetsov** discloses the device further comprising a storage media, the storage media operable to maintain a database of a plurality of signature files therein.[column 7, lines 62-67]

8. **As per claims 5-8, Kouznetsov** discloses the device as applied to claims above. Furthermore **Kouznetsov** discloses the device wherein the intrusion detection application identifies a correspondence between the signature file and a data packet, a determination that the data packet is intrusion-related made upon identification of the correspondence. [Column 7, lines 31-38]

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 11-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061) in view of **Smaha et al**, (hereinafter referred to as **Smaha)** (U.S. Patent No. 5,557,742)

11. **As per claims 11-13**, **Holland** discloses **a node** [figure 1, ref. Num "11"' ref. Num "12"] of a **network for managing an intrusion detection system**,[Column 1, lines 15-18; figure 1, ref. Num "20", ref. Num "19", ref. Num 18"] (The present invention relates in general to network intrusion detection data collection and, in particular, to a system and method for intrusion detection data collection using a network protocol stack multiplexor). **The node comprising**:

- **A memory module for storing data in machine readable format for retrieval and execution by the central processing unit**; [Column 4, lines 23-29]

  - **An operating system** [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**

  A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure 3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and

later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers) and

- **A media access control driver** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the "media access control driver", also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC) and **operable to execute an intrusion protection system** [Column 4, Lines 52-53;figure 2, ref. Num "37" and column 4, lines 31-32]

Holland does not explicitly discloses

- Management application, the management application operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, the node operable to transmit the signature file to a mobile device over a radio frequency link.

However, in the same field of endeavor, **Smaha** discloses

An application operable to receive text-file input defining a network-exploit [figure 1, ref. Num "20" and "12"; figure 5a, ref.Num "12"; column 4, lines 40-49] (For instance, input mechanism shown on figure 1, ref.

Num "20" receives input from any wide array of sources for example user devices shown on figure 1, ref. Num "22") and **convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, [figure 5a, ref. Num "144"; column 5, lines 10-12; Column 6, lines 9-11]** (The misuse engine shown on figure 1, ref. Num "30" converts the input into events/signature and compare it with the known signatures and generate a signature representative of an exploit-signature when detecting a misuse during processing operations and send it to the out put mechanism as shown on figure 5a, ref. Num "32") and **the node operable to transmit the signature file to a radio frequency link**.[column 6, lines 15-17; figure 1, ref. Num "36" and "38" and ref. Num "40"] (the output signal is sent to the communication links.)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of converting the input into events/signature and compare it with the known signatures and generate a signature representative of an exploit-signature when detecting a misuse during processing operations and send it to the out put mechanism as shown on figure 5a, ref. Num "32" and transmitting to the communication links as per teachings of **Smaha** in to the method of analyzing the traffic using signature-based and statistical-based intrusion detection techniques as taught by **Holland**, in order to create a system a system capable of automatically recognizing intrustions and misuses.(See Smaha, Column 3, lines 9-10)

12. **Claims 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Victor Kouznetsov** (hereinafter referred as **Kouznetsov**) (U.S. Patent No 6,725,377B1) **in view of Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061)

13. As per claim 2, **Kouznetsov** discloses a device or a method of monitoring intrusion using an anti-intrusion monitor server running Window NT operating system. [Column 6, lines 32-34]

Kouznetsov does not explicitly discloses

- The operating system further comprises a network stack comprising a protocol driver, a media access control driver, the intrusion detection application comprising an intermediate driver bound to the protocol driver and the media access control driver.

However, in the same field of endeavor, **Holland** discloses

An operating system [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**

A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure 3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer

shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers)

- **A media access control driver** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the "media access control driver", also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC) and

- **The intrusion detection system implemented as an intermediate driver [Figure 2, ref. Num "37"] and bound to the protocol driver** [figure 2, ref. Num "33"] and **the media access control driver.**[figure 2, ref. Num "31"] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num "37" is implemented as an intermediate driver and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83",

namely the network layer and the transport layer are all implemented by the protocol driver.)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the operating system as per teachings of **Kouznetsov** in to the method of operating system which comprises the network stack as taught by **Holland**, in order to relates network intrusion detection with respect to a network protocol stack.

Conclusion

14. **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
September 12, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100